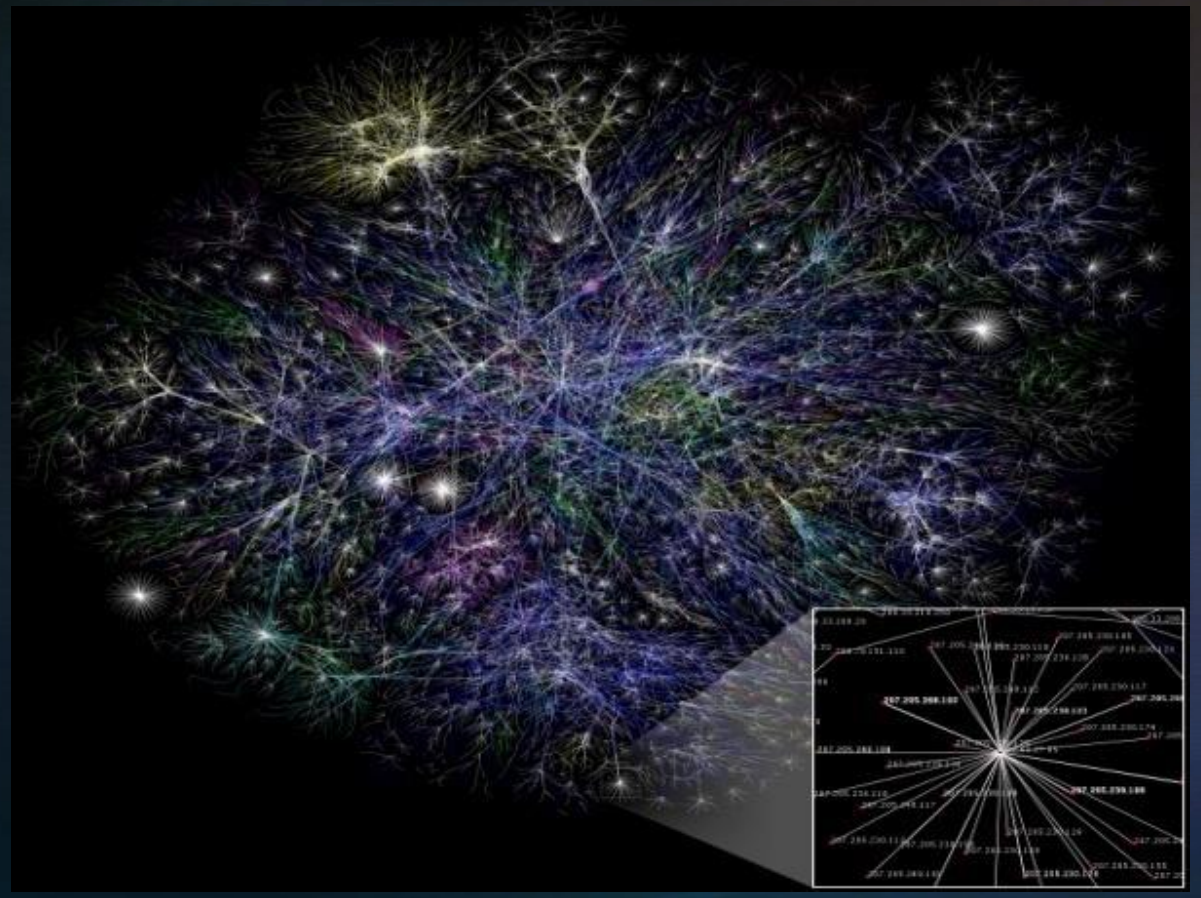
TCP/IP Networking in a Nutshell



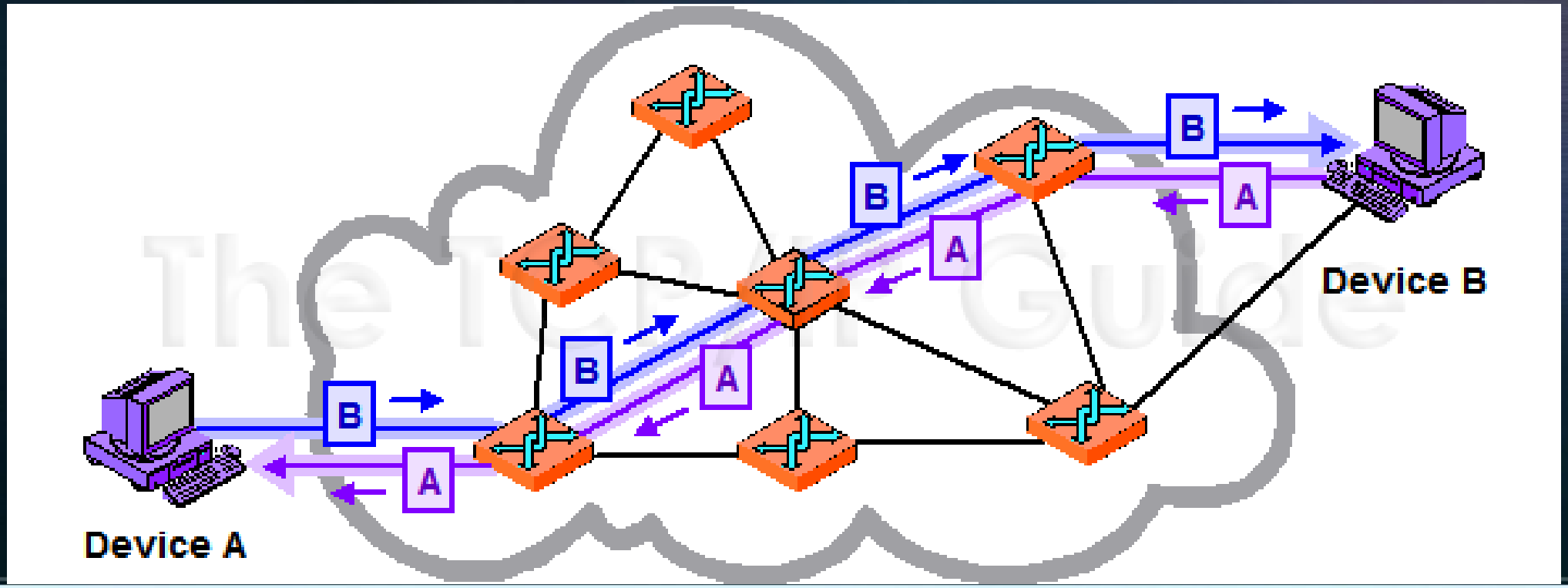
Kevin Cleary
MGS 650

The Internet

- The Internet is governed by a series of protocols that form the rules for how communications should happen
- The Internet is a network of networks.
  - There is no centralized point.
  - There are no boundaries.
- Information that is sent from one location on the internet to another is broken down into smaller, more manageable pieces called "packets".

Circuit (Message) Switching

- A means of connecting two devices in which there is a dedicated “line” or connection between the two devices.
- The established connection remains active for the duration of the message transmission.
- This is how the public switched telephone network works.

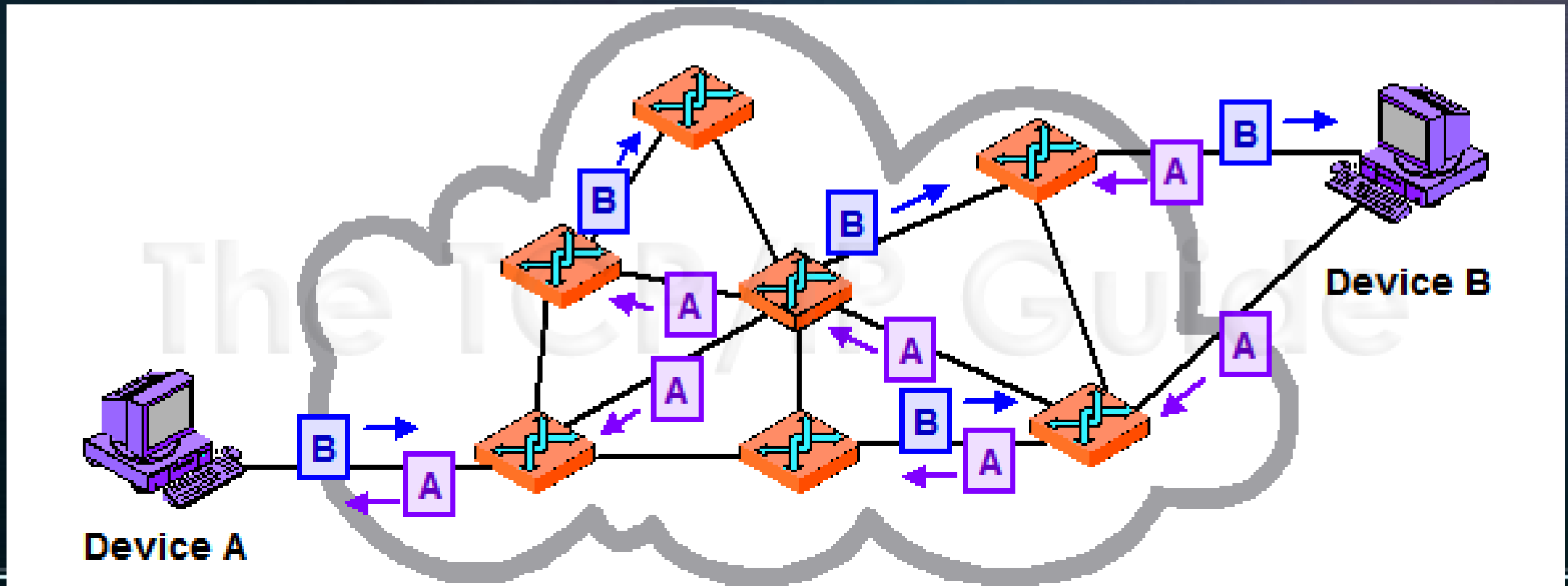


Circuit (Message) Switching

- Advantages:
  - Good for when communicated information must be received in order.
- Disadvantages:
  - This form of communication is very inefficient for computers.
    - Low Link utilization
  - A single failure anywhere along the communication path will stop all packet flow.

Packet Switching

- Packets are sent on their own, independently, to their destination.
  - Packets may take different routes.
  - Packets may arrive out of order.
  - A small number may not even arrive.
- Packet switching does not require a dedicated communications circuit.



Packet Switching

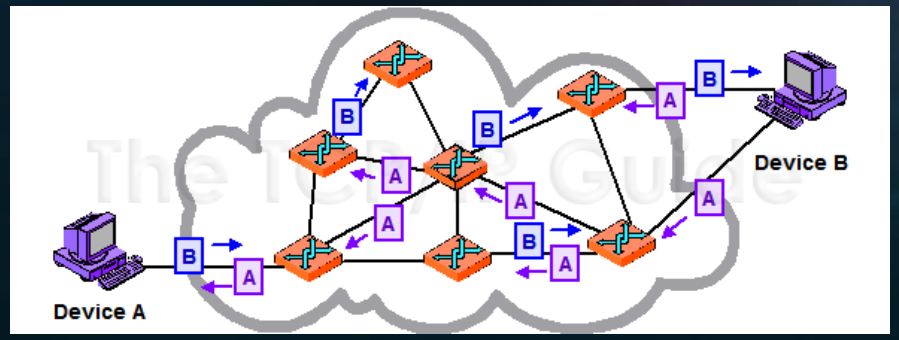
- Advantages:
  - More tolerant to failures
  - Better utilization of an internet connection
- Disadvantages:
  - Packets may arrive out of order
  - Packets may not arrive at all!
  - Controlled chaos from a messaging perspective

Packet Vs Circuit Switching

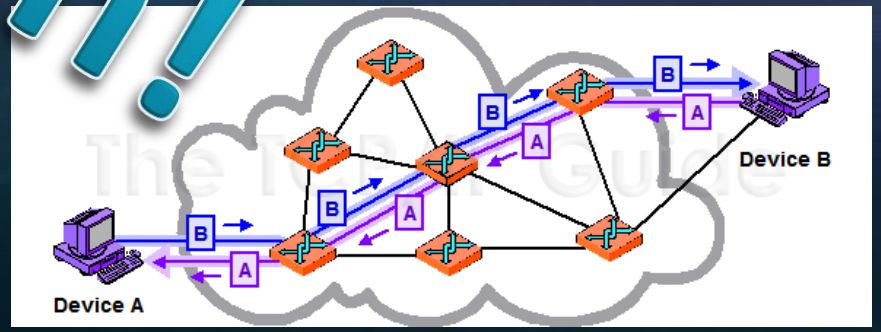
Which form of communication is better?

Both!

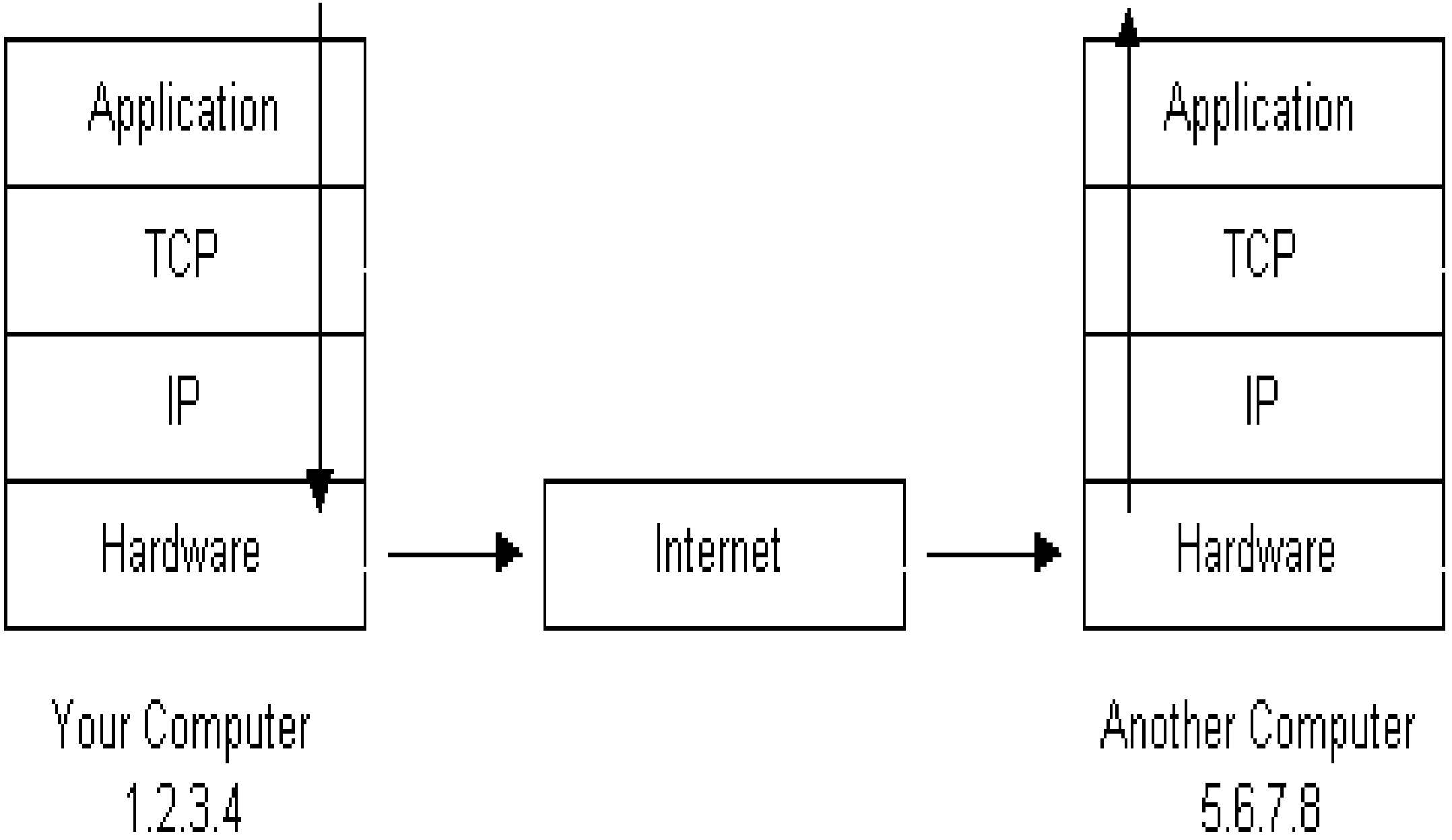
Packet Switched



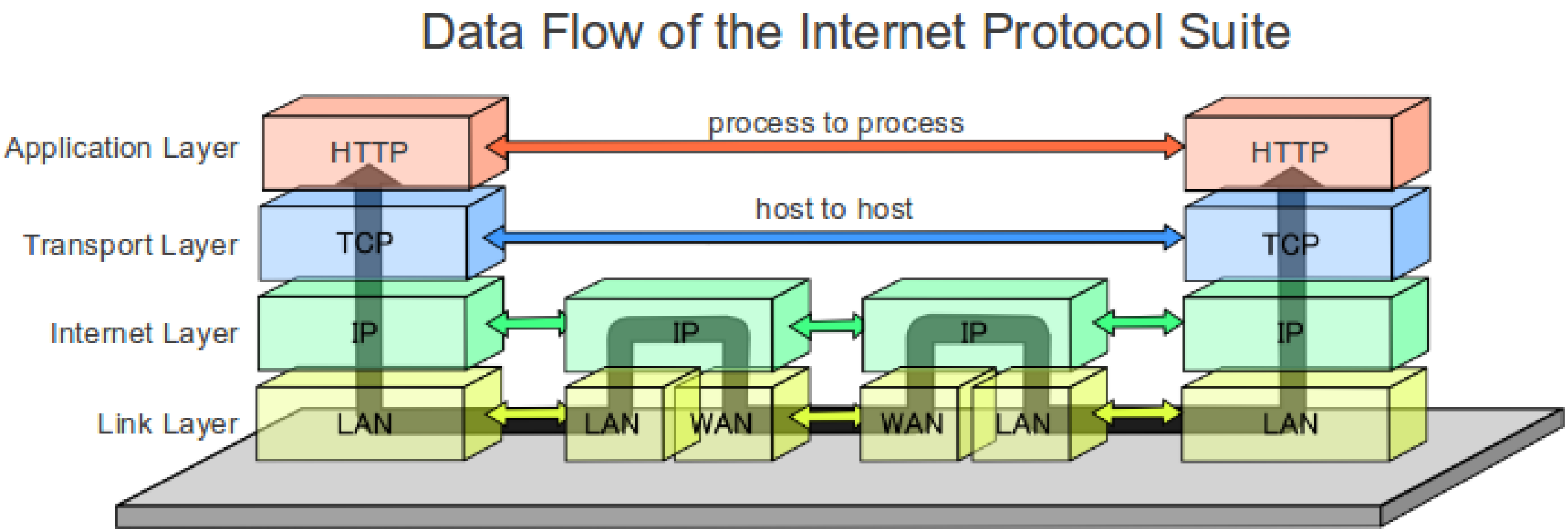
Message Switched



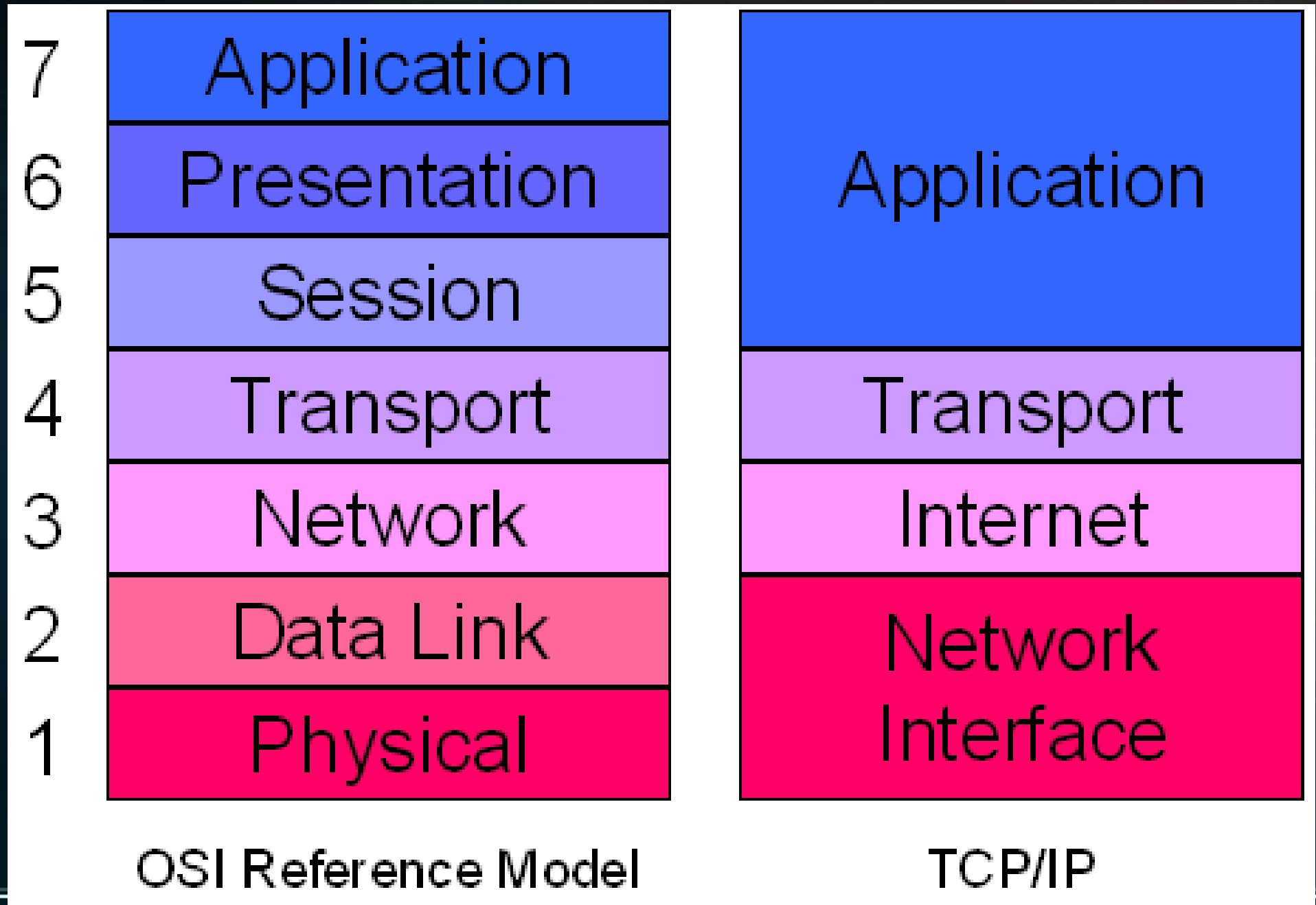
Protocol Stacks



Protocol Stacks



The OSI Stack

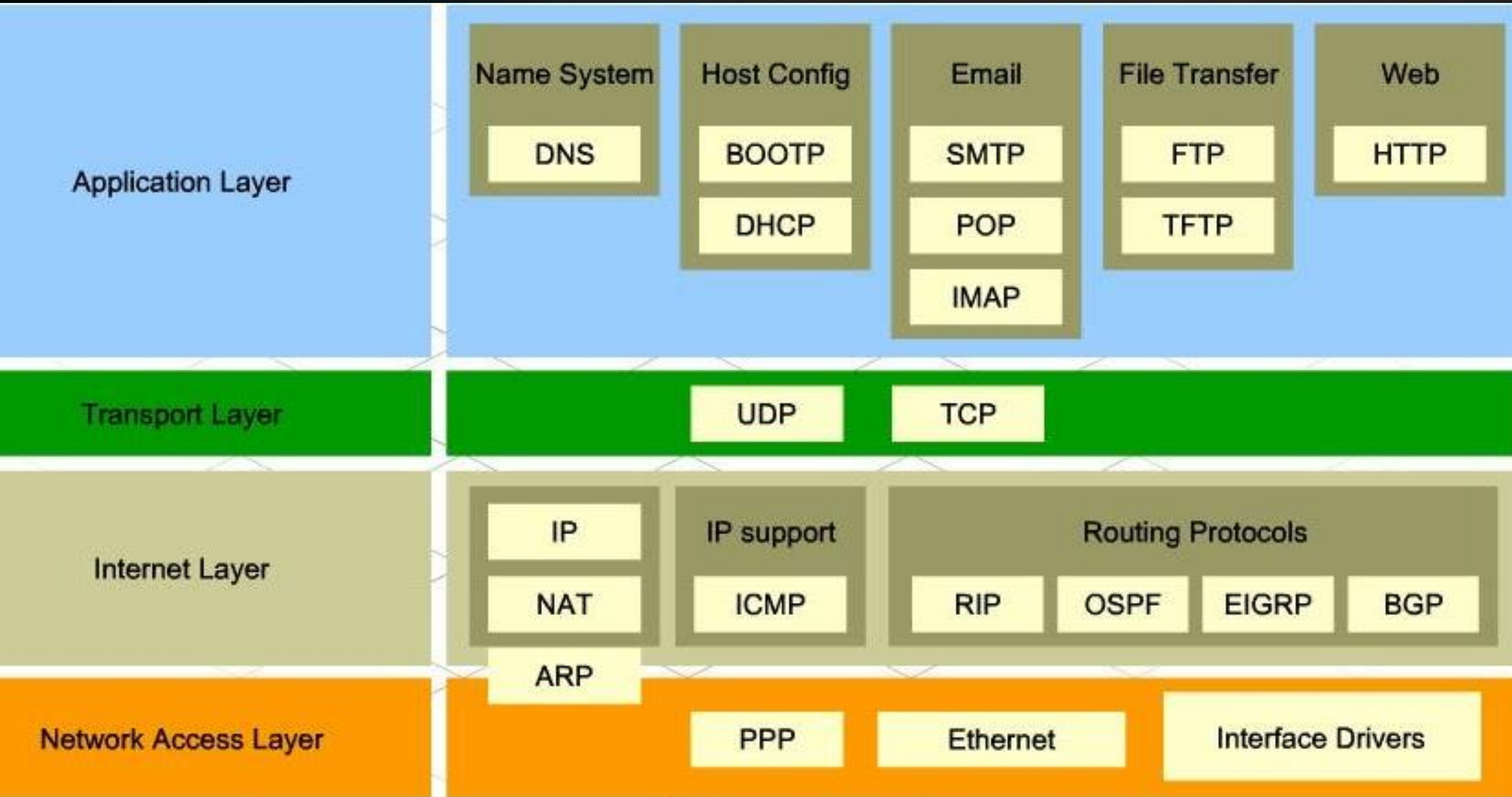


Protocol Stacks

- The protocol stack used by every computer on the Internet is known as TCP/IP.
- The stack includes:
  - Internet Protocol (IP)- packet switched
  - Transmission Control Protocol (TCP)- Circuit switching
- The TCP/IP protocol stack takes care of how computer communications get routed to the correct computer and how the applications assemble and make sense of newly arrived packets.

Protocol Stacks

- When an applications whishes to send a message over the Internet it hands the message off to the protocol stack. Each protocol within the stack has some task.
- Your application passes information on to the TCP layer to be broken up in to manageable chunks called packets.
  - Information is added to the packet headers for re-assembly.
    - Sequencing numbers
    - Session IDs
- The IP layer takes care of steering these packets.
- The Hardware physical transmits packets (frames).


Application Layer
Name System
DNS
Host Config
BOOTP
DHCP
Email
SMTP
POP
IMAP
File Transfer
FTP
TFTP
Web
HTTP
Transport Layer
UDP
TCP
Internet Layer
IP
NAT
ARP
IP support
ICMP
Routing Protocols
RIP
OSPF
EIGRP
BGP
Network Access Layer
PPP
Ethernet
Interface Drivers

The TCP Layer

- The Transmission Control Protocol (TCP) takes care of breaking application information in to chunks, known as “packets” and assigning those packets information such as:
  - Port number - help to separate what data is destined to which applications.
    - Email and Web browsers have a specific, unique port number
  - Number of packets sent
  - The number the packet in the series being sent.
  - On the receiving end the TCP protocol helps to arrange packets as they arrive in the correct order for the applications.

Protocol Stacks

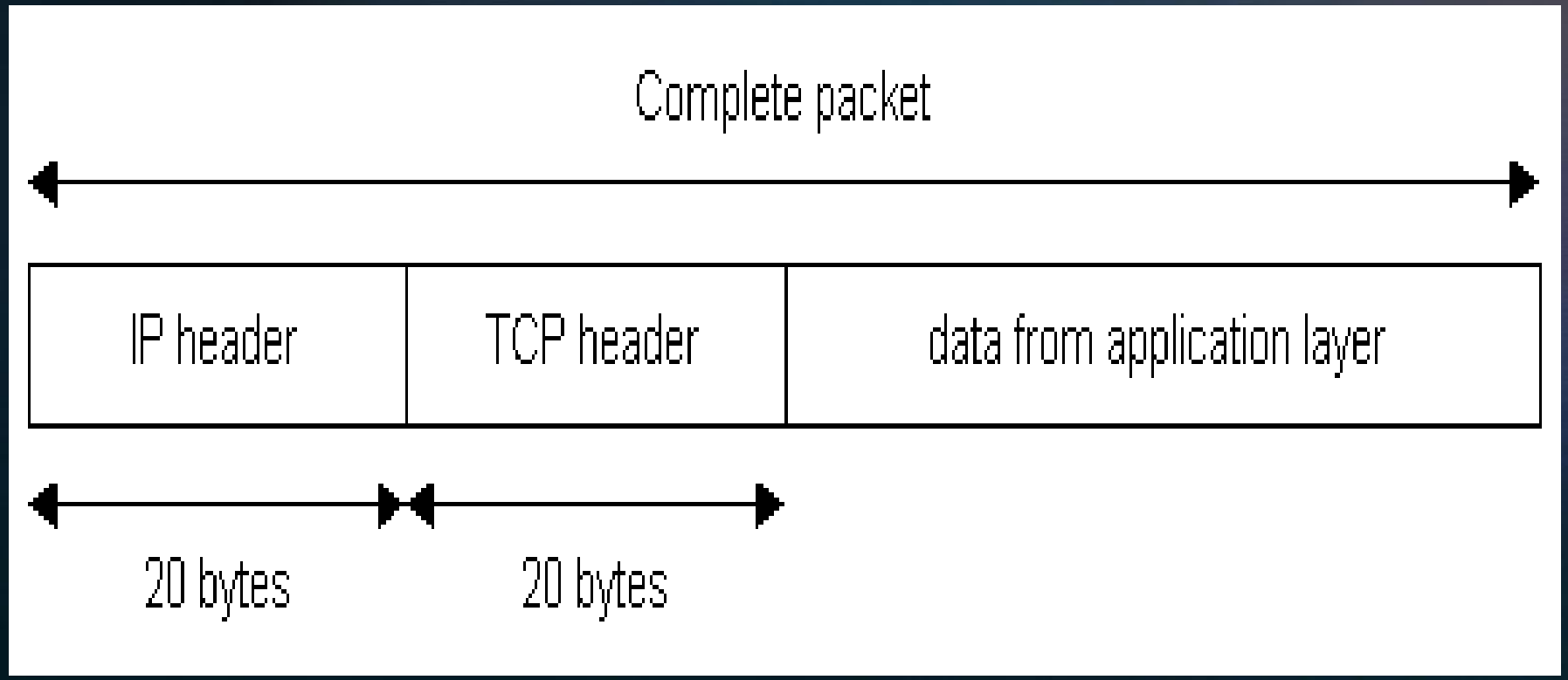
- TCP is a connection-oriented, message switched, reliable, byte stream service.
  - Connection-oriented means that two applications using TCP must first establish a connection before exchanging data (a handshake).
  - TCP is reliable because for each packet received, an acknowledgement is sent to the sender.
  - A cousin of TCP, User Datagram Protocol (UDP) is commonly used for streaming.
    - A connectionless, unreliable protocol

Protocol Stacks

- IP is an unreliable, connectionless, packet switched protocol.
  - IP's job is to send and route packets to other routers / computers.
  - IP packets are independent entities and may arrive out of order or not at all.
  - IP does not guarantee packet delivery.
  - A series of diagnostic tools exist at the IP layer, the Internet Control Messaging Protocol ICMP.
    - Popular tools include “ping” and “traceroute”.

Protocol Stacks

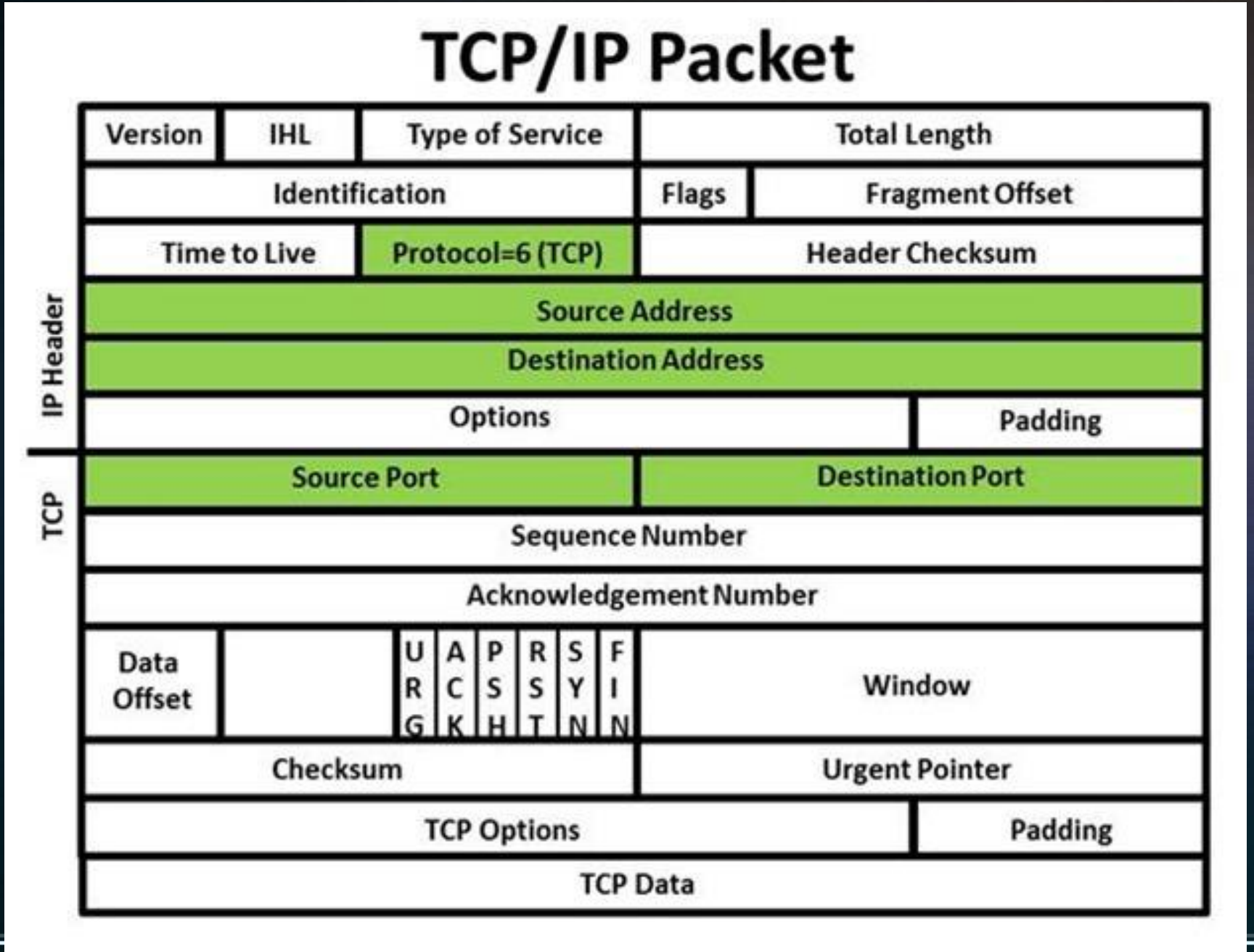
- Each layer places its information in the “packet header”.
  - This is information needed to deliver and re-order the packet once it has arrived to its destination.



Packet Routing at the IP Layer

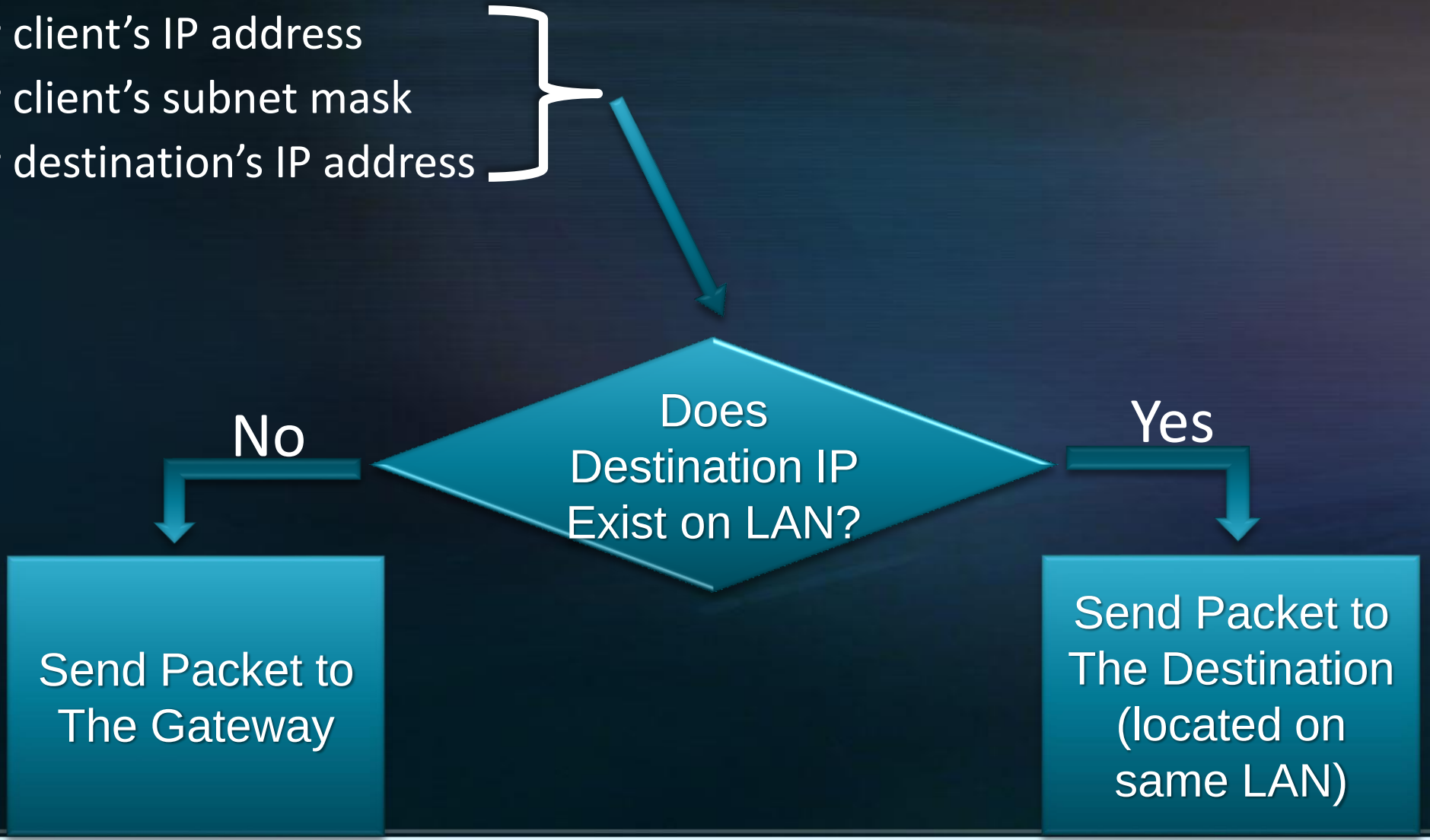
- IP packet routing is similar to mailing a letter.
- The steps you take in mailing a letter include…
  - Sealing your message in to an envelope.
  - Looking up the address to write on the envelope.
  - Determine if you can hand deliver your message or if it needs to be given to the mail man.
  - If the mailman must deliver the message you must hand the message off to them. The mailman works with other mailmen to then deliver your envelope.
  - Wait for a response.

Protocol Stacks



The Flow of Internet Data

- The IP layer determines if the client your sending a packet to resided on you LAN by looking at:
  - Your client's IP address
  - Your client's subnet mask
  - Your destination's IP address



IP Client Information

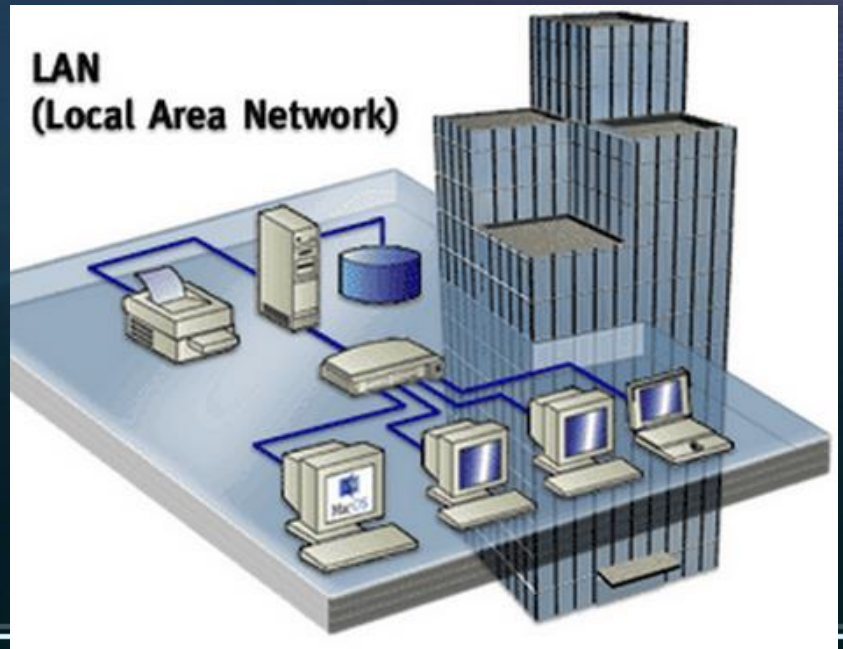
- For the IP layer to route packets correctly, a device must be configured with:
  - IP address: Every IP address on the internet is unique. An address takes the form of:
    - 4 x 8 bit (32 bit) numbers represented in decimal notation separated by ‘.’s. For example 128.205.34.66. – IPV4
    - 8 x 16 bit (128 bit) alphanumeric addresses in decimal notation separated by ‘.’s. For example 2001:0000:3238:DFE1:63:0000:0000:FEFB – IPV6
    - IP addresses (To and From) are placed in packet headers, similar to how one would label an envelop.
  - Subnet Mask – used to determine the boundaries of a Local Area Network (LAN).
    - A subnet mask resembles an IP address. Ex 255.255.255.0
  - Gateway IP Address – where packets destined for outside our LAN are handed off.

The Flow of Internet Data

- Gateways will communicate with one or more other gateways and devices called “routers”.
  - Routers are usually connected between subnets and take care of handing off massive amounts of packets.
  - Gateways make convenient locations for Firewall and Monitoring measures.
- Routers maintain multiple connections to one another.
- Routers constantly keep track of other routers around them.
  - They will look at things like:
    - link speeds
    - delay times
    - network congestion.
  - Routers are connected to “backbones”. Backbones are the information super highways of the internet.
- Routers have a role in security but are not security devices.

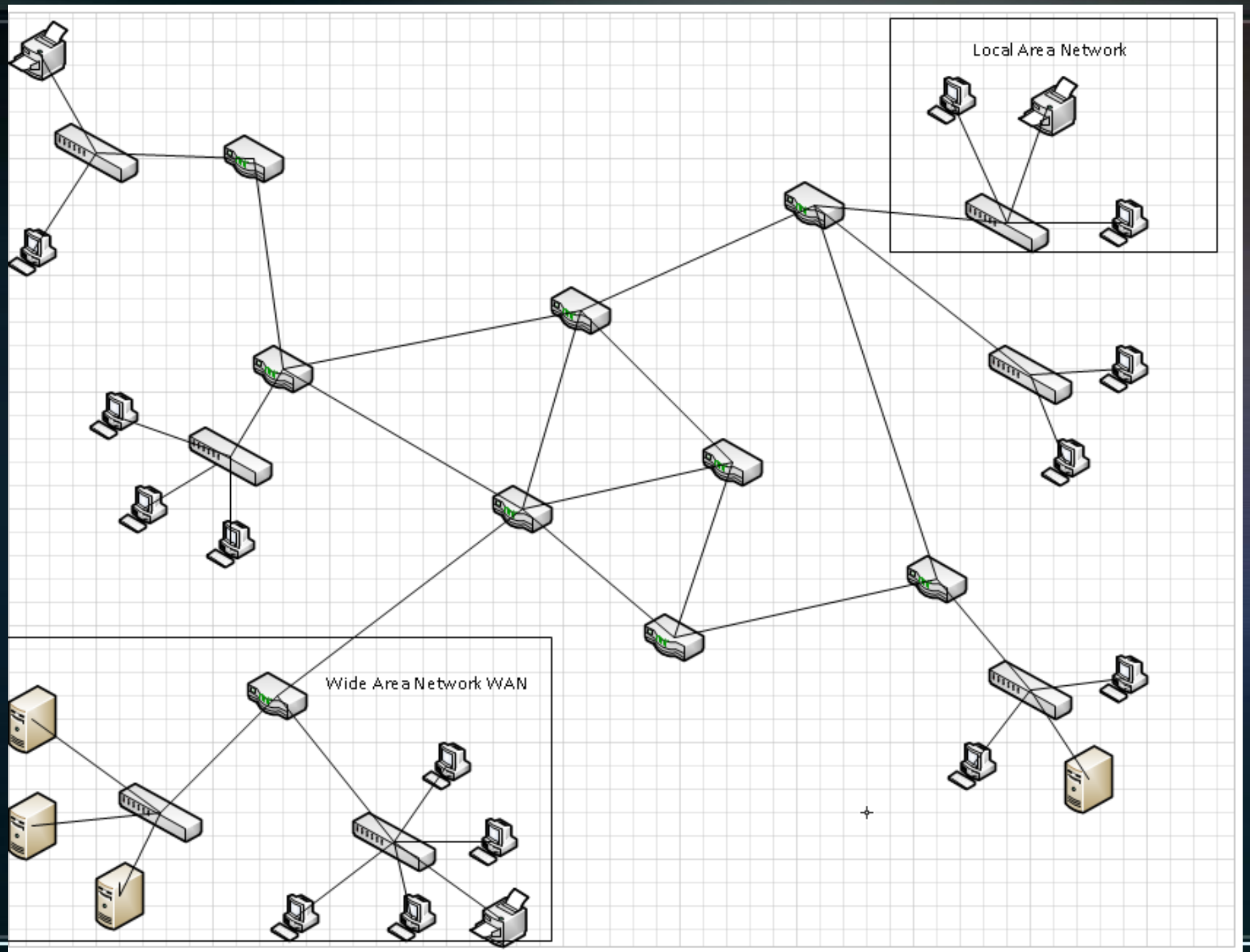
Local Area Networks

- LANs are the most basic type of network.
  - These small networks are the building blocks of the Internet.
  - Can be thought of as a “local neighborhood” of computers or devices
  - All devices on the same LAN communicate directly with one another across a “switch” (collision domain).
  - LAN communication DOES NOT require a gateway.
  - Network and LAN segmentation is a **fundamental security concept**.
    - LANs can be organized by :
      - Geographic area
      - Device type / Function
      - Administrative boundary
      - Data or work classification
      - Department or entity



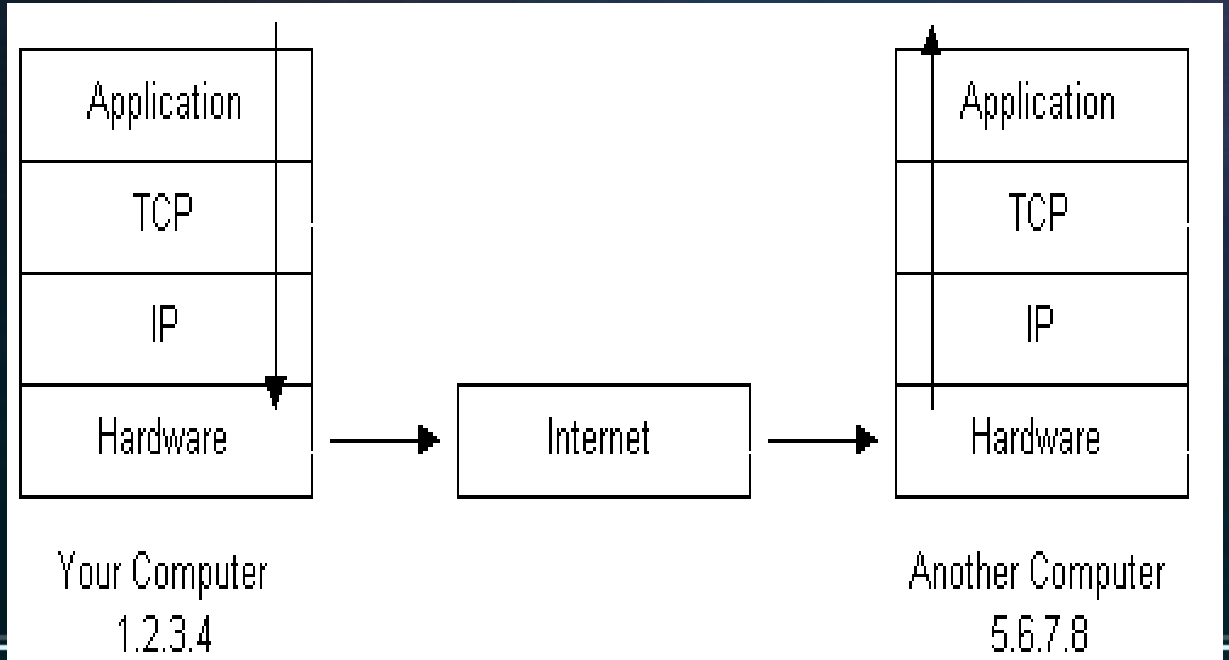
Wide Area Networks

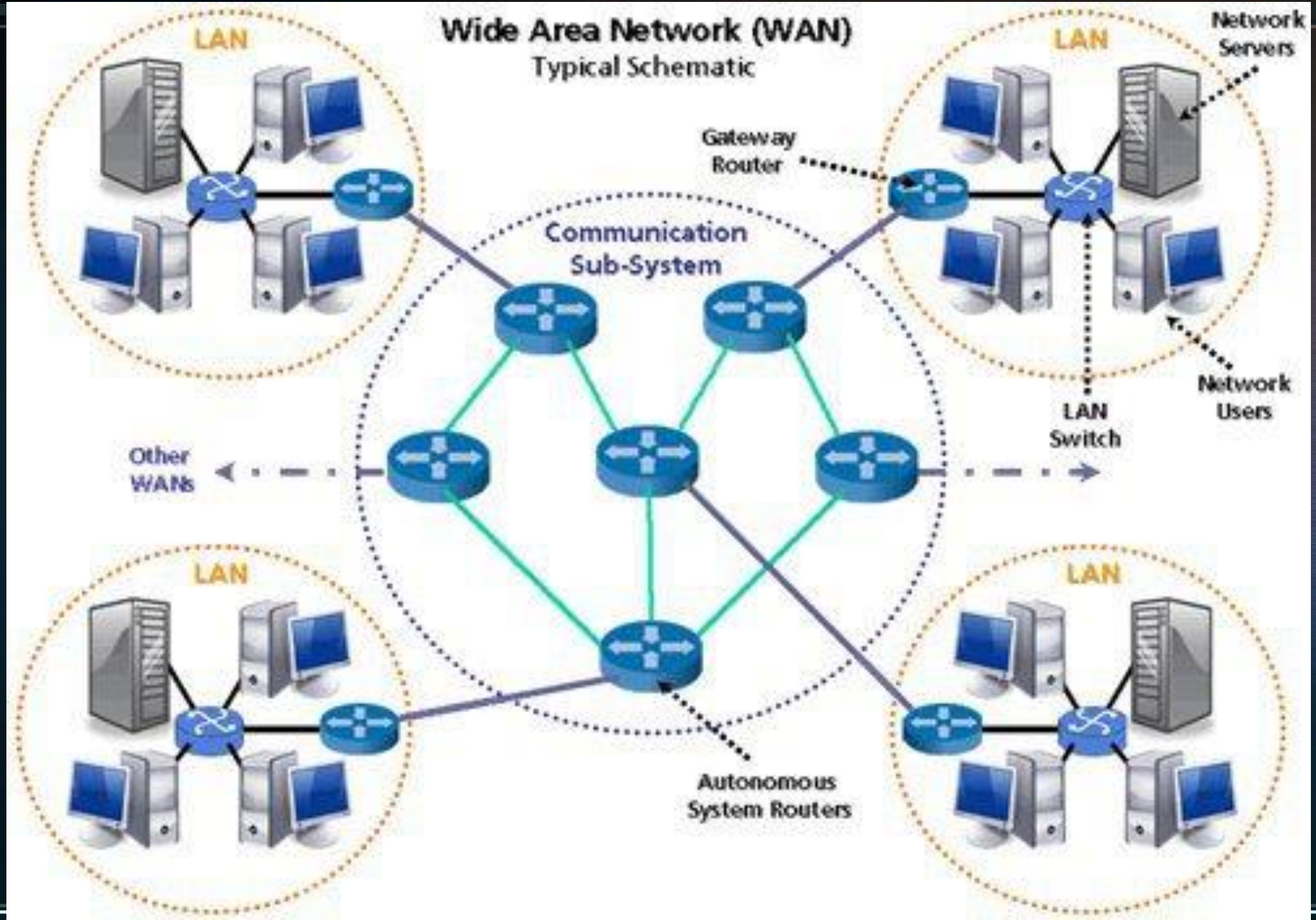
- LANs are connected together to form WANs
  - LANs get connected to WANs through routers.
  - The “Internet” is one big WAN.
  - We can connect LANs to WANs through both wireless and Wired Connections.
  - WANs can span much larger geographic distances than LANs.


Local Area Network
Wide Area Network WAN

The Hardware Layer

- The “hardware“ layer (sometimes called the “Link Layer”) of the internet is in charge of transmitting data over a physical medium.
- The physical medium for transmitting data can take on many forms and is implemented with a wide variety of technologies, both wired and wireless.




Wide Area Network (WAN)
Typical Schematic
LAN
LAN
Network Servers
Gateway Router
Communication Sub-System
Network Users
LAN Switch
Other WANs
LAN
LAN
Autonomous System Routers

Connecting It All

	LANs	WANs
Wired	Ethernet (NICs and Switches) • 1 GB/S • 10GB/S	Modem DSL/ISDN Cable Fiber Optic
Wireless	Wifi (802.11 B/G/N/AC)	Satellite (Microwaves) 4G (Cell service) Infra-red

Connecting to LANs - Ethernet

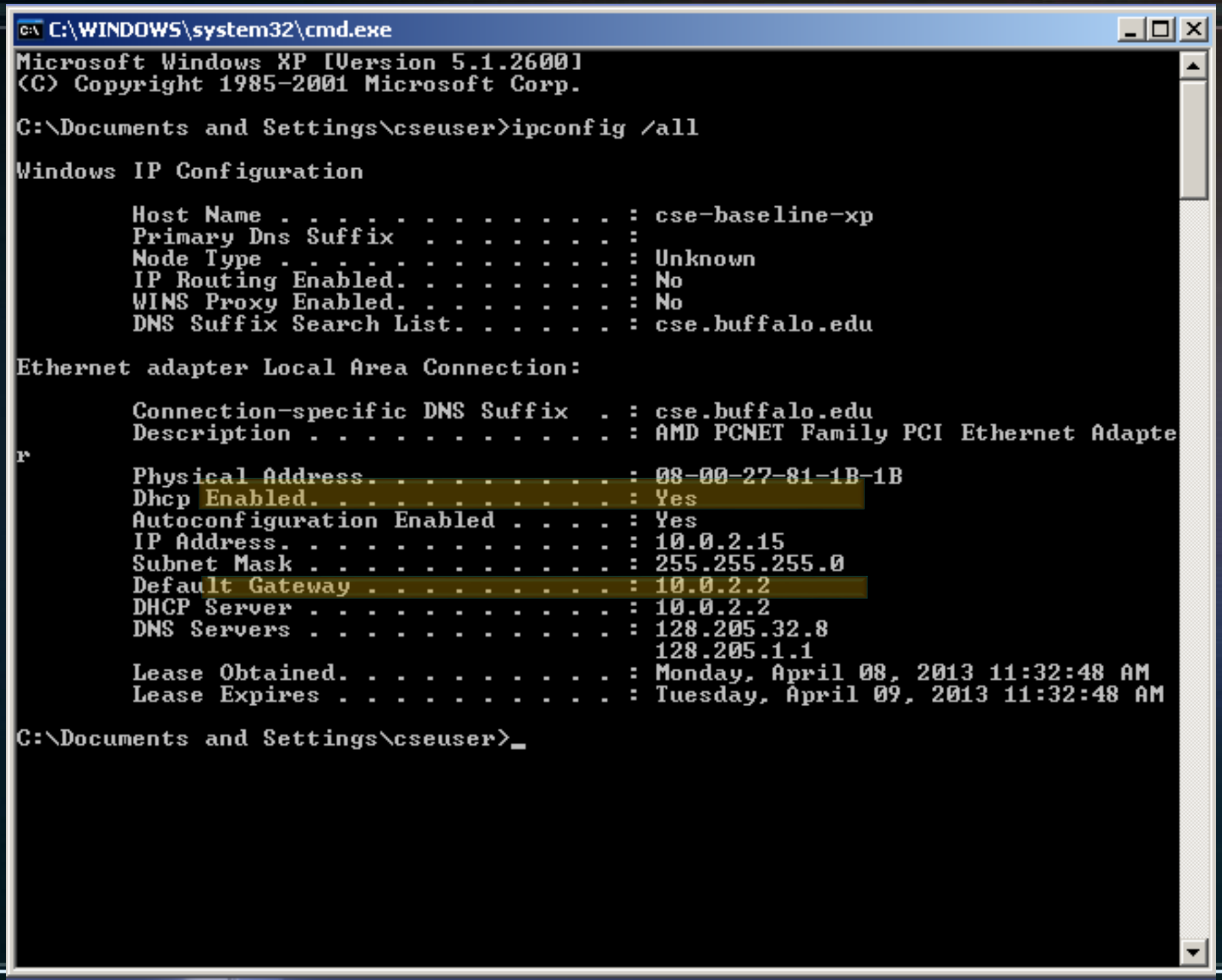
- Ethernet can be thought of as:
  - Hardware communication devices
  - Topologies of devices being used
- Common Ethernet speeds are around 1000Mb/s (1000Base-T) also called gigabit.
- Most Ethernet devices such as network interface cards and switches have the ability to negotiate the highest available speed.
- Power over Ethernet (PoE) allows the transmission of power through an Ethernet network cable. This is useful for things like VOIP phones.

Connecting to LANs - Ethernet

- Switches - devices that physically connect multiple computers together to form a subnet.
  - Switches use a star topology and work by joining electrical pathways together, so that devices can talk to each other.
  - Hubs look similar to switches but use a ring topology, relying on each member node to pass along a packet of information.
  - More advanced switches support Virtual Local Area Networks, VLANS, SPANing, TAPing, port filtering, etc…

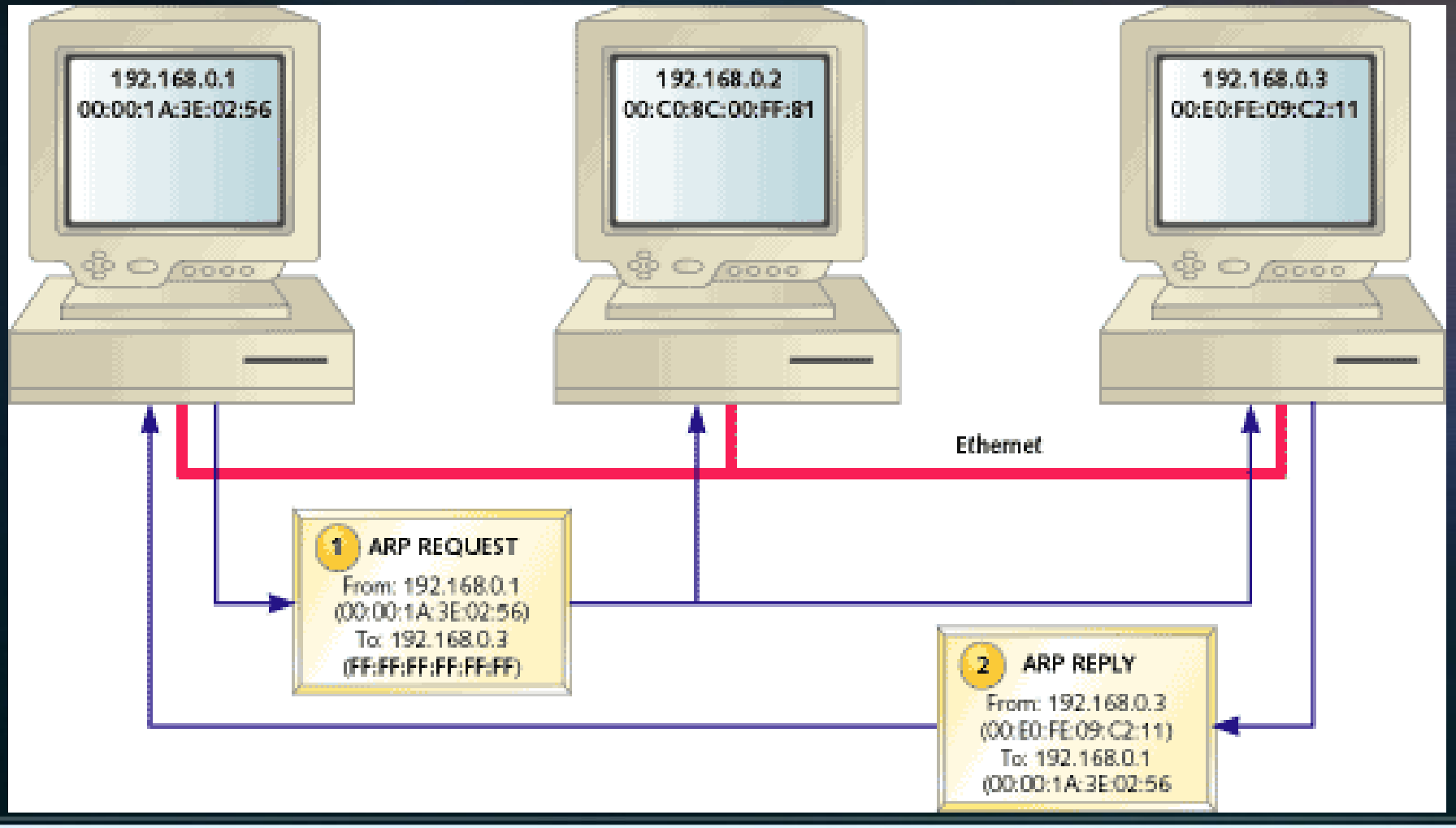
The Hardware Layer

- All machines have a Hardware address called a “MAC” address, or “Media Access Control Address”.
  - address is hardcoded on the network interface card (NIC) and usually cannot be changed.
  - The MAC address is used when delivering messages along a subnet.
- It is possible for a MAC address to have multiple IP addresses bound to it.
- The binding between MAC and IP address is handled through “Address Resolution Protocol” (ARP).


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\cseuser>ipconfig /all
Windows IP Configuration
Host Name . . . . . : cse-baseline-xp
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : cse.buffalo.edu
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : cse.buffalo.edu
Description . . . . . : AMD PCNET Family PCI Ethernet Adapte
r
Physical Address. . . . . : 08-00-27-81-1B-1B
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.2
DHCP Server . . . . . : 10.0.2.2
DNS Servers . . . . . : 128.205.32.8
128.205.1.1
Lease Obtained. . . . . : Monday, April 08, 2013 11:32:48 AM
Lease Expires . . . . . : Tuesday, April 09, 2013 11:32:48 AM
C:\Documents and Settings\cseuser>

The Hardware Layer

- Your machine will only use ARP to communicate with other devices on your own subnet.

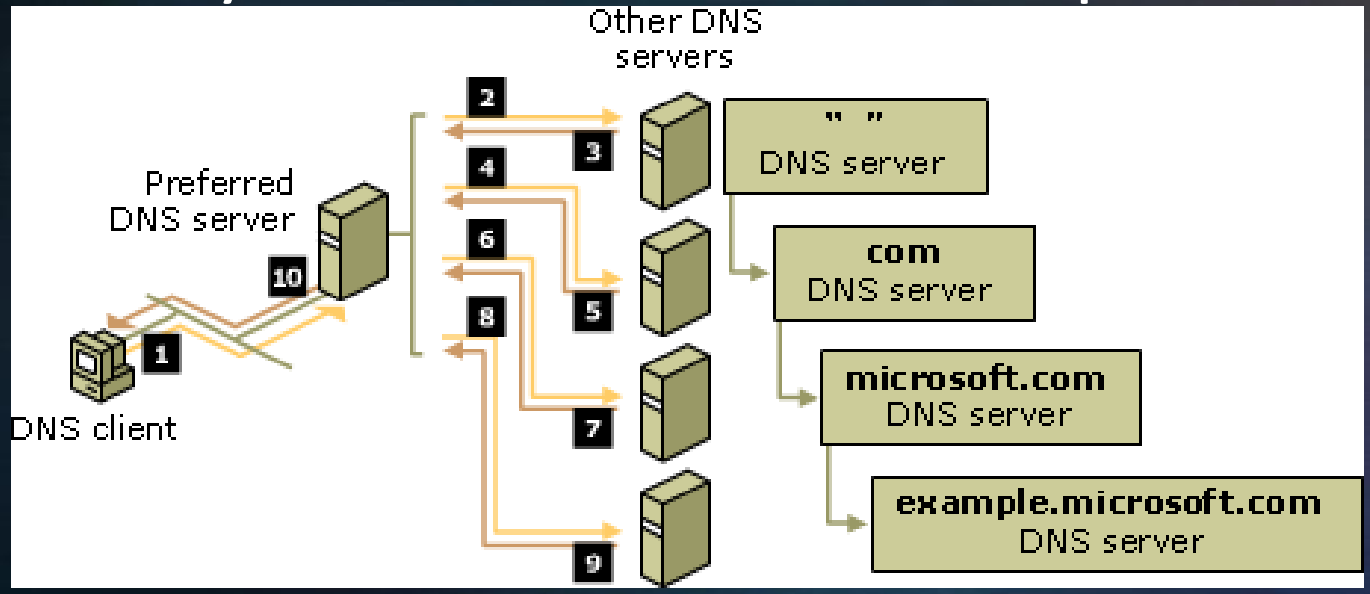


Domain Name System (DNS)

- Translate domain names such as “google.com” to IP addresses
  - It’s easier to memorize and type domain names than IP addresses.
- Getting a domain name involves registering the name you want with an organization called the “Internet Corporation for Assigned Names and Numbers” (ICANN) through a domain name registrar.
- Consider www.google.com
  - .com is called the “top level domain”.
  - Google is the second level domain.
  - www is the host name.
- Domain Name lookup is an iterative process.
  - Doman Name servers are arranged in a hierarchal fashion, ex: www.bbc.co.uk
  - Distributed sub-domain servers all manage small portions of IP addresses.
  - There are 12 root servers globally that resolve top level domain names.

Domain Name System (DNS)

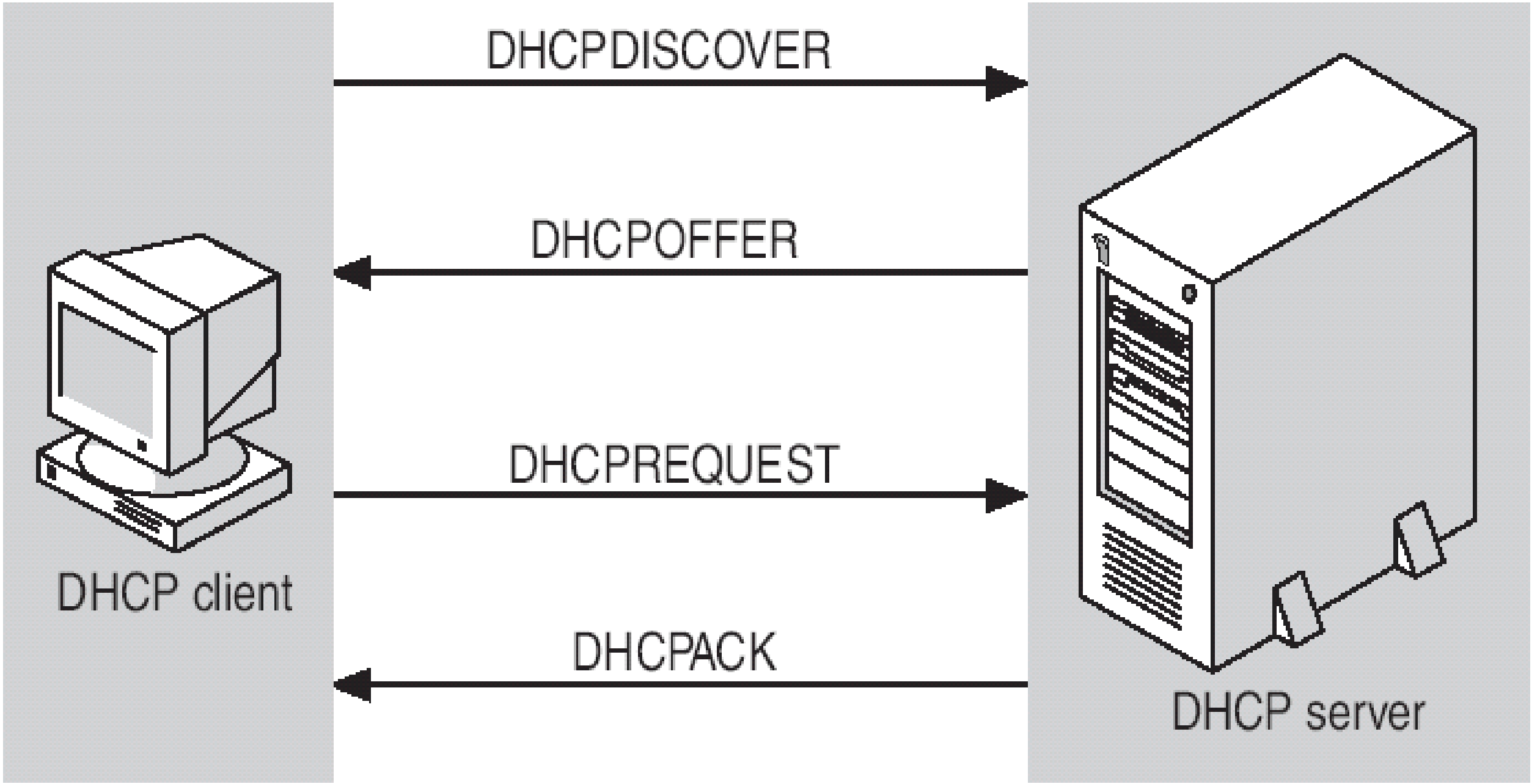
- A local DNS server will temporarily cache entries for greater speed upon subsequent lookups.
- Each name server only knows of its own small portion of its domain.



- DNS is an connectionless protocol
- DNS has been weaponized in recent years with what are called amplification attacks.

Dynamic Host Control Protocol (DHCP)

- Server addresses are said to be "**static**".
  - These addresses do not change over time and are manually set by someone.
- Workstations tend to have "**dynamic**" addresses.
  - These addresses are managed or "leased" by a central authority (DHCP)
- DHCP will set all the network parameters your device needs in order to communicate on a network.
  - IP Address
  - Gateway Address
  - Subnet Mask
  - DNS Servers
  - Other valuable information*
- DHCP hides details of the IP protocol and network setup from users.
- When you connect to a network your computer asks that network's DHCP server for the needed network information.


DHCPDISCOVER
DHCPOFFER
DHCPREQUEST
DHCPACK
DHCP client
DHCP server

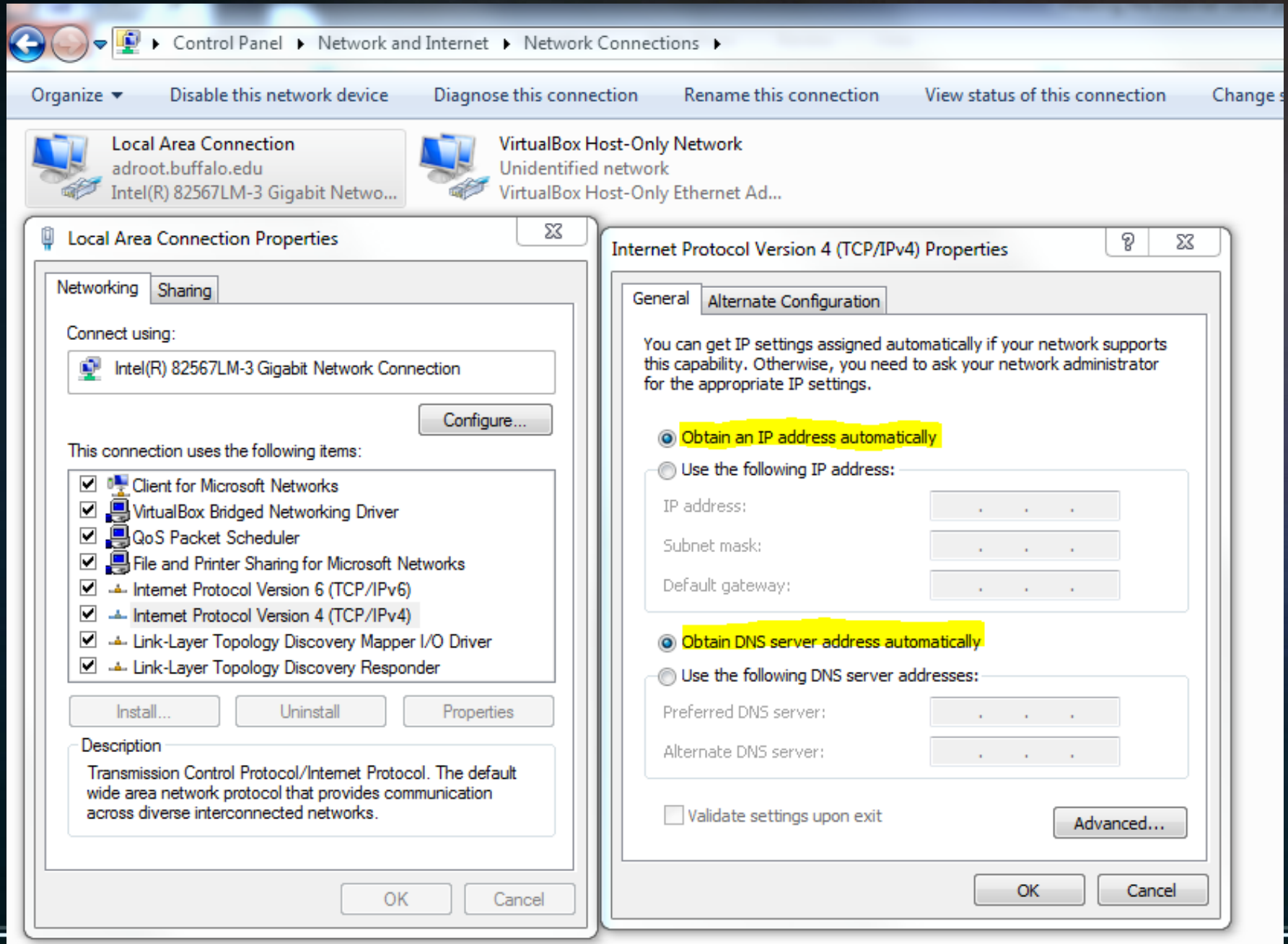
Dynamic Host Control Protocol (DHCP)

- A new client broadcasts a DHCP discover message to a local subnet.
- A DHCP server responds with a DHCP offer message that contains an IP address for lease to the client.
- When the offer message is received, the client selects the offered address by replying to the server with a DHCP request.
- The offering server sends a DHCP acknowledgement message (DHCPACK) , approving the lease.
  - Other DHCP option information is included in the acknowledgement.
  - Once the client receives acknowledgment, it configures its TCP/IP properties using the information in the reply

Dynamic Host Control Protocol (DHCP)

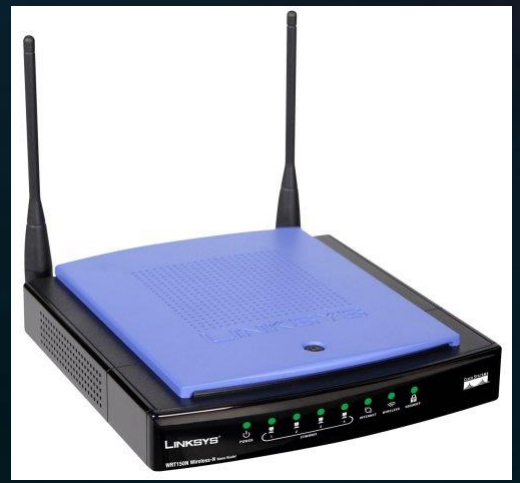
- What happens when :
  - There is no server to answer your request?
    - Your client will guess its own address and assign an “Automatically Assigned IP Address” (AAIPA).
    - You will know this is happening if your machines IP address starts with a “169….”.
  - The wrong DHCP server answers?
    - This could be a type of attack known as a “Rogue DHCP”.
    - A bad guy could route traffic through a malicious host.

Dynamic Host Control Protocol (DHCP)



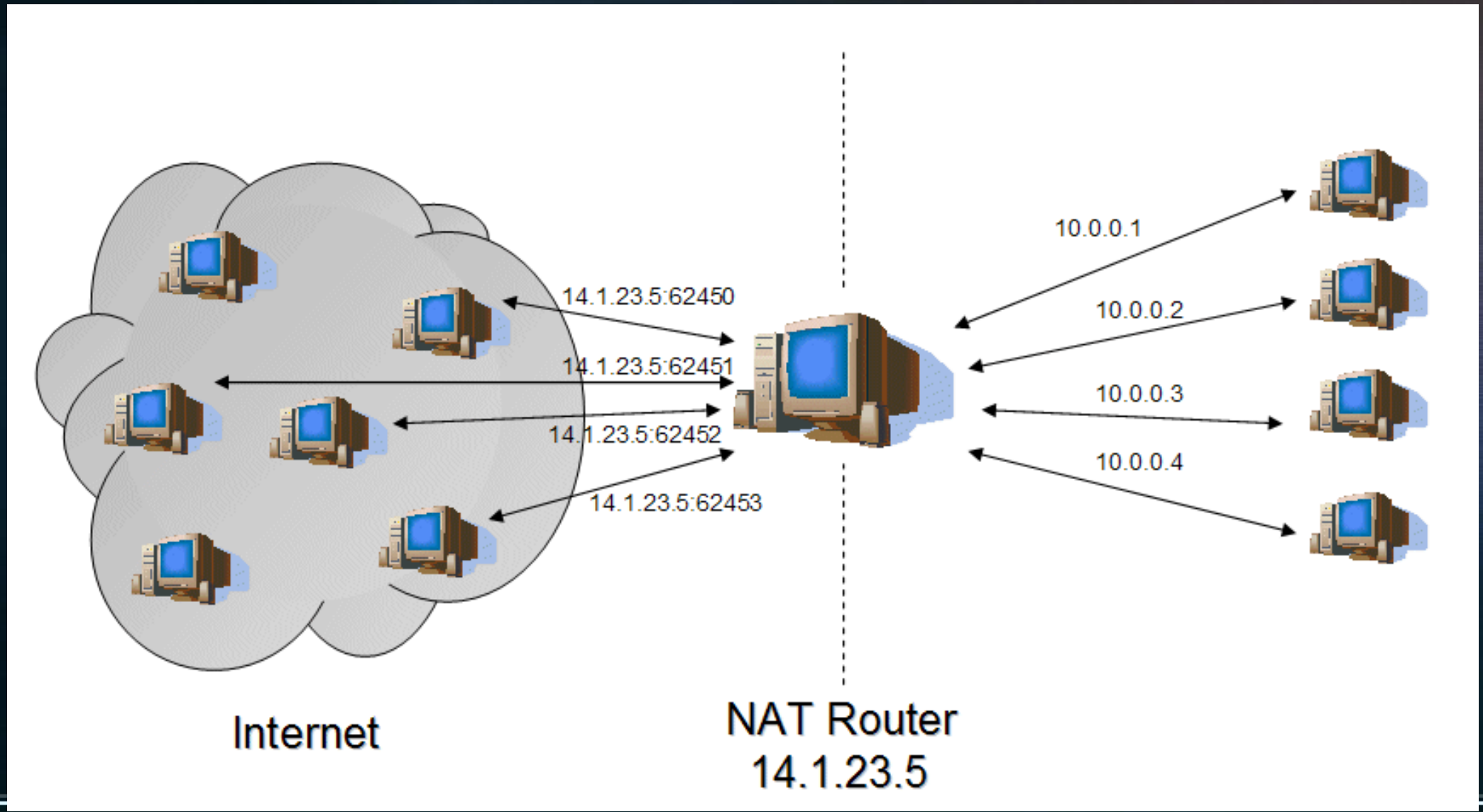
Home Networks

- What are home routers?
  - A Switch?
  - A Gateway?
  - A Firewall?
  - A Server?
  - A DSL/Cable Modem?



Home Routers

- Most Home Routers will function as a Network Address translation Firewall, or NAT.

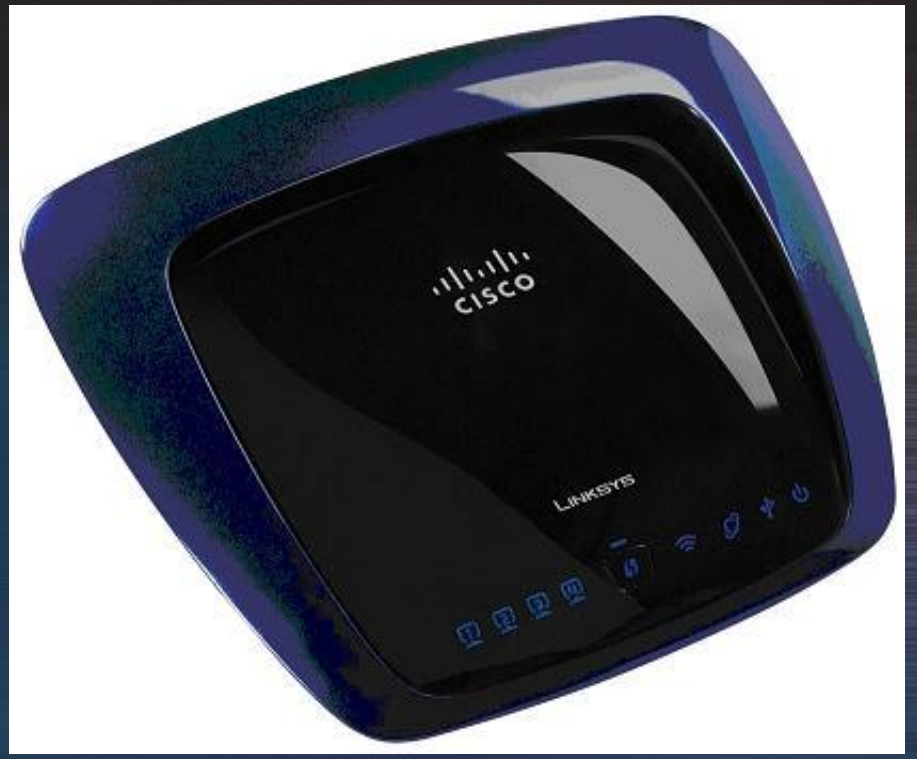


Home Routers

- Most Home Routers will function as a Network Address Translation Firewall (NAT).
  - NAT allows a single device, such as a home router, to act as an agent between the Internet (public network) and a local (private) network.
  - Only a single, unique, IP address is required to represent an entire group of internal or private computers, such as a home network.
  - In a home setup, a NAT firewall allows several home devices to share a single IP provided by an ISP
  - NATs help to hide the internal setup of your network.

Home Networks

- Home Routers provide a combination of:
  - IP address routing (gateway)
  - Network address translation (NAT)
  - DHCP functions
  - DNS
  - Firewall functions
  - LAN connectivity like a Network switch
  - Modem Functionality
  - Some allow you to connect an external USB or E-Sata drive as a means of providing shared storage.



Home Networks

- Home Routers are connected to the internet through an Internet Service Provider (ISP).
  - An ISP provides you a way to connect to their own WAN, providing access to the Internet.
  - An ISP will provide you a modem or home router to connect through their preferred transmission medium.
    - Sometimes these devices must be connected to a local switch to form your own LAN